Optimizing video surveillance solutions with IBM Cloud Object Storage, Tiger Bridge, and Genetec Security Center

A technical report

Overview

Challenge

How do you minimize the online storage requirements and realize the cost savings based on the data life cycle of the video surveillance solutions?

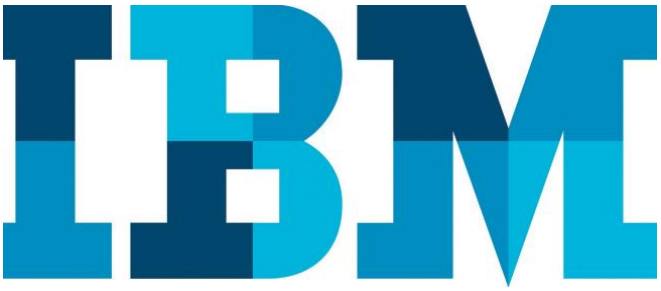
Solution

This paper provides the configuration and sizing guidelines for transparent data movement between the online storage and on-premises private or hybrid cloud storage using Tiger Bridge connector and IBM Cloud Object Storage.

The objective of this paper is to minimize the online storage requirements with transparent data tiering to the on-premises private cloud storage or hybrid cloud storage in the digital video surveillance solution. The paper covers the test strategy used and the results of the testing. This paper describes the solution architecture for deploying Genetec security solutions on IBM Cloud Object Storage with Tiger Bridge. This paper provides recommendations, and configuration and tuning adjustments to help ensure an efficient installation of the joint solution with acceptable performance that meets the needs of the organization.

Genetec Security Center video management software is a powerful surveillance platform that is easy to manage. Security Center is the unified security platform from Genetec that blends IP security systems within a single intuitive interface to simplify your operations. The configuration capabilities of the software design enable you to customize the solution to fit your exact needs.

IBM® system engineers thoroughly tested the solution using the system parameters outlined in this paper. This technical white paper covers the test results that describe the configuration of the Genetec Security Center server running on IBM Storwize® systems with Tiger Bridge and IBM Cloud Object Storage. It illustrates the hardware impact (on the processor, storage, and network) when changing the individual parameters of the video surveillance system, and provides recommendations on how to configure the surveillance system for optimal performance.



Storwize family summary

- Three Storwize V5000 hybrid models—IBM Storwize V5030, IBM Storwize V5020, and IBM Storwize V5010
- 2U rack-mountable chassis
- 1 Gb iSCSI, 12 Gb SAS and 16 Gb Fibre Channel or 10 Gb iSCSI/Fibre Channel over Ethernet host ports
- Small form-factor enclosure: Twenty-four 2.5-inch drives
- Large form-factor enclosure: Twelve 3.5-inch drives
- Up to 504 drives per system and up to 1,008 drives with two-way clustered systems
- Up to 2 PB per system and 4 PB with two-way clustered systems
- RAID 0, 1, 5, 6 and 10 and distributed RAID support for fault tolerance.
- 32 GB cache standard (64 GB cache optional); 128 GB with two-way clustered systems
- Redundant, hot-swappable power supplies and fans

Assumptions and prerequisites

This solution paper assumes that users are equipped with the following technology skills prerequisites:

- Proficiency in installing and configuring the Genetec Security Center
- Familiarity with installing and configuring the IBM Storwize storage and IBM Cloud Object Storage solutions.
- Proficiency in installing and configuring the Microsoft® Windows® operating system.

The configurations documented in this paper are based on the tests conducted in the IBM internal lab. These results might differ from individual production implementations in the field.

IBM Storwize V5000 family

IBM Storwize V5000, built with IBM Spectrum Virtualize™ software, includes a highly flexible, easy to use, all-flash or hybrid storage solution that provides improved performance and enterprise support. The Storwize system includes the following features:

- Provides mid-range customers with a cost-effective, scalable storage platform that can provide advanced features typically only available to more expensive enterprise-class products
- Delivers a new, easy-to-use graphical interface to access all the features of the platform
- Provides automated tiering capabilities with the IBM System Storage Easy Tier® function, can move the frequently accessed extents to high-performing flash storage.
- Provides multiprotocol support for Fibre Channel (FC) and Internet Small Computer Systems Interface (iSCSI) attachment
- Enables replication over IP to improve network utilization for remote mirroring with innovative technology

Tiger Bridge

Tiger Bridge key features

- Runs on Windows 7, Windows 10, or Windows Server 2008/2012 R2
- Is installed as add-on software on existing file servers
- Has no impact on the server performance
- Does not need to crawl the file system to detect ongoing changes
- Works with standard NTFS file systems
- Supports native Active Directory authentication
- Is capable of full and partial retrieval
- Is optimized for high performance environments
- Is capable of restoring lost file system metadata from target
- Supports a wide variety of object-based storage, such as:
  - Native S3 protocols
  - Amazon AWS
  - DataDirect Networks WOS
  - IBM Cloud Object Storage

Tiger Bridge can minimize your online storage requirements with Transparent Data Tiering. Tiger Bridge is a secure and flexible software connector for the Windows OS that transparently replicates and moves the data from a local volume to a cloud or on-premises target—without affecting users, applications, or workflows. As such, it allows organizations to better match their storage technology with their data lifecycle in order to realize substantial cost savings

Tiger Bridge dynamically reclaims space on a fast primary server by decommissioning its stale data to a slower, more economical tier of storage. Capacity requirements for high-speed storage is therefore greatly reduced while the longevity of valuable data is increased by being stored on more appropriate, lower cost technology. Best of all, Tiger Bridge can be installed within minutes on active servers without affecting users, applications, or workflows.

Using advanced data replication and space reclaiming technology, Tiger Bridge keeps the right data at the right place at the right time. By analyzing access to files and by relying on simple policies, such as last access date, file size, and free space that should be retained on the primary server, Tiger Bridge determines when a newly created or updated file must be replicated or when a stale file must be archived. Users and applications are not affected when files are migrated from the primary server to the secondary tier, because a stub-file is created to replace the file that was moved. Stub-files are distinctive and contain all the valuable metadata information of the original file (such as size, permission, last access date, and so on) and can be accessed by users and applications similar to any other file. When a stub-file is accessed, the original file is automatically and transparently restored back to the primary server and handed to the application, just as normal. Users and applications therefore do not experience any disruption in their workflow. And because it runs directly on your Windows server and manages your existing NTFS file system, you do not need to reformat the storage, give up performance, or compromise security by going through an external gateway server. Data gets moved between your primary and secondary tiers of storage. When connecting to a target over the S3 protocol, data gets encrypted directly on the server, before it is sent to the cloud, thereby ensuring the highest level of security.

IBM Cloud Object Storage

IBM Cloud Object Storage highlights

- Scalability that offers a single storage system and namespace versus an ever-increasing number of limited-capacity storage silos
- Security features that include a wide range of capabilities designed to help meet security requirements
- Reliability and availability characteristics of the system that are configurable to best suit customer requirements
- Manageability that helps enable storage administrators to handle large storage capacity
- Flexibility of a defined storage solution that does not require specific or proprietary hardware

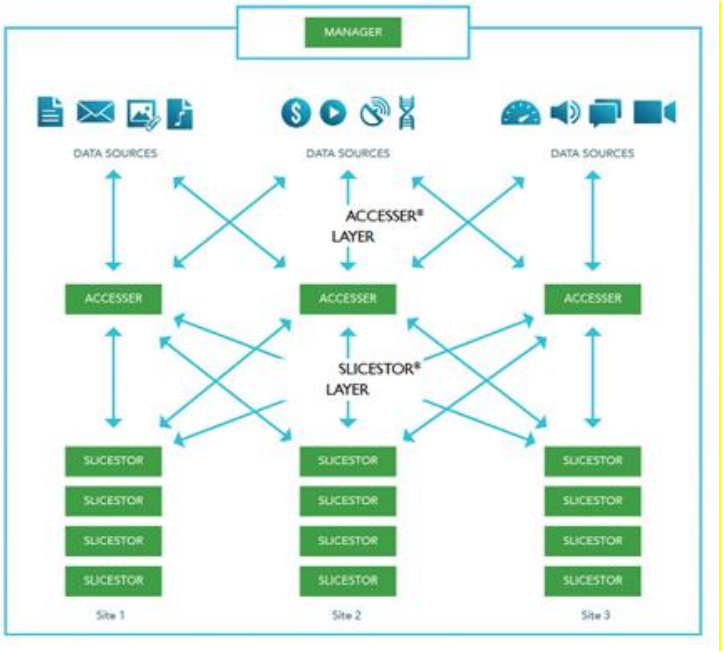


Figure 1: IBM Cloud Object Storage System

The IBM Cloud Object Storage System™ uses an innovative approach for cost-effectively storing large volumes of unstructured data while helping ensure security, availability, and reliability. IBM Cloud Object Storage technology uses Information Dispersal Algorithms (IDAs) to separate data into unrecognizable *slices* that are distributed through network connections to storage nodes locally or across the world. The collection of distributed storage appliances creates what is called an IBM Cloud Object Storage System. With IBM Cloud Object Storage dispersed storage technology, transmission and storage of data are inherently private and secure. No complete copy of the data resides in any single storage node, and only a subset of nodes needs to be available in order to fully retrieve the data on the network.

The IBM Cloud Object Storage System enables the creation of storage systems using three software components – the IBM Cloud Object Storage Manager, IBM Cloud Object Storage Accesser and IBM Cloud Object Storage Slicestor. These software components can be deployed on a wide range of compatible industry-standard hardware platforms, as virtual machines, and in the case of the IBM Cloud Object Storage Accesser, as an application running on a Linux® OS. Physical and virtual deployment can be combined in a single system, for example, virtual machines for the IBM Cloud Object Storage Manager and the IBM Cloud Object Storage Accesser and physical servers for the IBM Cloud Object Storage Slicestor.

Key lab components

- IBM Storwize V5030
- Tiger Bridge
- IBM Cloud Object Storage
- Genetec Security Center 5.2
- Brocade Fibre Channel switch
- VMware ESX hypervisor
- 10 Gb Ethernet switch

Each of the following three software components serves a specific function as a part of IBM Cloud Object Storage:

- The IBM Cloud Object Storage Manager is responsible for monitoring the health and performance of the system, configuring the system and provisioning storage, managing faults, and other administrative and operational functions.
- The IBM Cloud Object Storage Accesser is responsible for encrypting or encoding data on ingest and decoding or decrypting data when read as well as managing the dispersal of data slices resulting from this process across a set of IBM Cloud Object Storage Slicestor nodes.
- The IBM Cloud Object Storage Slicestor is responsible for the storage of data slices.

IBM Cloud Object Storage delivers the following features and benefits:

- **Availability**: Data is always available–whether or not there is planned or unplanned downtime.
- Scalability: Systems are easily able to grow from terabytes to petabytes to exabytes.
- **Security**: Data confidentiality is maintained even when multiple drives, servers, containers, or locations are compromised.
- **Economics**: The need for costly replication is eliminated, significantly lowering the total cost of ownership for storage systems at the petabyte level and beyond.
- **Efficiency**: More easily manage tens of petabytes of storage per administrator.

Solution key components

This section provides the details about the components used in the solution.

Genetec video management software

Video management software is the key component of a video surveillance solution that collects video data from the cameras and other data sources. Genetec Security Center is a leading software designed to provide the security solutions required for the large enterprise systems.

Key components:

- Directory role provides a centralized configuration database for all entities in the Security Center system.
- Omnicast is the IP video management component of Genetec Security Center.
- Omnicast requires additional server to host the archiver and media router roles.
- Archiver manages the communication with IP camera and storage system. It records up to 300 Mbps of throughput per server.

Lab configuration

Genetec directory server

- Two virtual processors, 16 GB memory, one 10 Gb Ethernet and Windows 2008 R2.

Genetec archive server

- Four virtual processors, 32 GB memory, one 10 Gb Ethernet and Windows 2008 R2
- 15 TB VDisk storage space from Storwize V5030
- Tiger Bridge connector for transparent data movement

Camera network

- Genetec Protocol Unit Simulator for camera ingesting
- Maximum 100 Mbps per simulator
- Three workstations for 300 camera simulation

Storwize V5030

- Dual controller with 16 Gbps FC Storage connectivity
- 15 TB VDisk from NL-SAS drives
- Multipath host mapping

IBM Cloud Object Storage

- One Manager device
- Three Accesser devices
- Nine Slicestor devices
- 1.7 PB raw capacity

Server platform

Server platform plays a key role in centralized surveillance systems as Omnicast archiver is limited to 300 Mbps. Hypervisors such as VMware helps to host multiple archivers on one physical server depending on the processor and memory resources.

Storage system

Storage system is the critical component in the surveillance system for storing video content. Simplicity, scalability, and affordability are the important considerations for storing huge volumes of video archives. IBM Storwize system provides a cost-effective platform for the online storage. Tiger Bridge provides a secure and flexible connector for transparent data movement between online IBM Storwize systems and the on-premises private or hybrid IBM Cloud Object Storage system. This architecture allows organizations to place the data on the appropriate storage tier based on the data lifecycle and helps in reducing the storage cost.

Networking

10 Gb Ethernet connectivity between the server platform, incoming camera network, and Genetec Security Center applications is recommended.

Lab validation configuration

The following hardware was used in the lab for validating the functionality and sizing information for the IP video surveillance solution using IBM Storwize system.

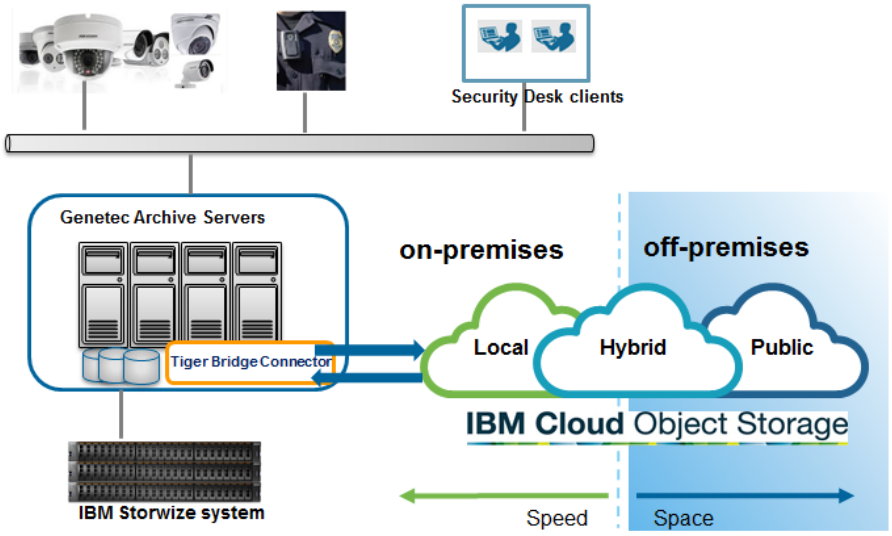


Figure 2: Genetec high-level architecture with IBM Cloud Object Storage

No.	Role	Configuration
1	Genetec directory server	Two processor core, 8 GB memory Windows 2008 R2, Genetec Security Center 5.2, Security Desk client for playback
2	Genetec archiver server	Four processor cores, 32 GB memory, 10 Gb Ethernet Windows 2008 R2, Genetec Security Center 5.2 archiver role, external 24-drive nearline (NL) serial-attached SCSI (SAS) RAID6 volume, NTFS file system with 64 KB storage allocation unit. Tiger Bridge connector software for transparent data movement between online IBM Storwize and IBM Cloud Object Storage.
3	Camera simulator	One processor core, 8 GB memory, 10 Gb Ethernet Windows 2008 R2, Genetec Protocol Unit Simulator
4	Storage unit	IBM Storwize V5030, Spectrum Virtualize software version 7.7.0, 24 drives RAID6 NL-SAS 7000 rpm for video storage unit.
5	Cloud storage	IBM Cloud Object Storage system with one Manger device, three Accesser devices, and nine Slicestor devices. It was configured with 1.7 PB raw capacity

Table 1: Lab configuration details

The virtual machines (VMs) were configured with windows 2008 R2 for the directory, archiver, and simulator servers.

Cameras: Genetec simulators were used for simulating video workloads. Three VMs, each configured up to100 cameras, are used for simulating a 300-camera data ingestion.

10 Gb Ethernet network was used for ingesting the video data from the camera network to the Genetec servers.

Testing and lab validation

Various tests were conducted in the lab with the focus on the storage-related factors for video archiving. A controlled environment was used for testing by adjusting the camera settings, and quantity of simulated cameras while monitoring key performance metrics for write latency, processor consumption, network utilization, and video frame loss.

The Genetec Protocol Unit Simulators utility was used to simulate the cameras. Tests were also performed after the system had run for a period of four days with the initial benchmark value and some amount of data had accumulated in the archive database, in order to simulate a production environment. Through the Genetec Protocol Unit simulation utility, the camera count was set at 300 cameras per archive server and ran for four days, without loss of frame data.

The test procedure includes the following steps:

1. Configure the IBM Storwize V5030 system as the video storage.

Figure 3: IBM Storwize V5000 login page

2. Configure the archive role server as the Fibre Channel host on the IBM Storwize system.
3. Create RAID6 NL-SAS storage volumes and assign them to the archiver servers as the video storage.

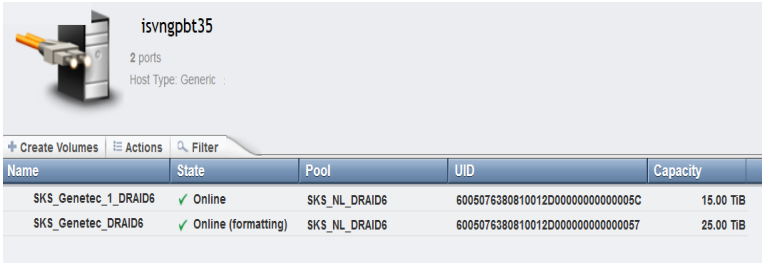


Figure 4: IBM Storwize volumes

4. Configure three servers for simulating the camera data ingestion. Configure each server to simulate up to 100 Mbps camera data.
5. Configure the archive role server with the video storage space from the IBM Storwize system.

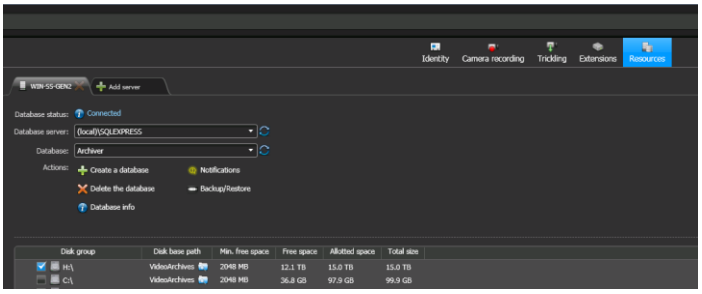


Figure 5: Genetec archiver configuration

6. Configure video units to produce the required camera traffic ingestion to the archiver.

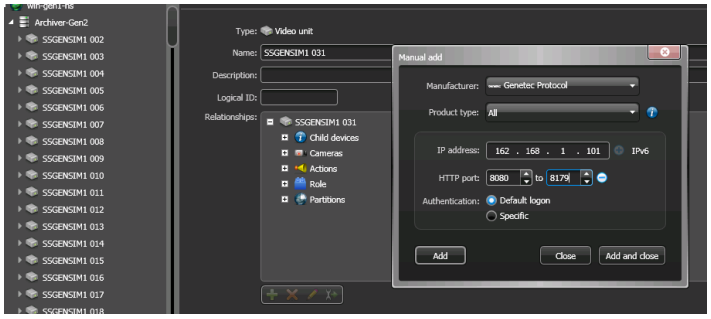


Figure 6: Genetec camera unit configuration

7. Configure motion detection on all the cameras.

8. Install and configure the Tiger Bridge connector software on the Genetec archiver server for transparent data movement between online storage and cloud storage.

9. Create a vault on IBM Cloud Object Storage for archiving the content from the genetic archiver server to the cloud storage.

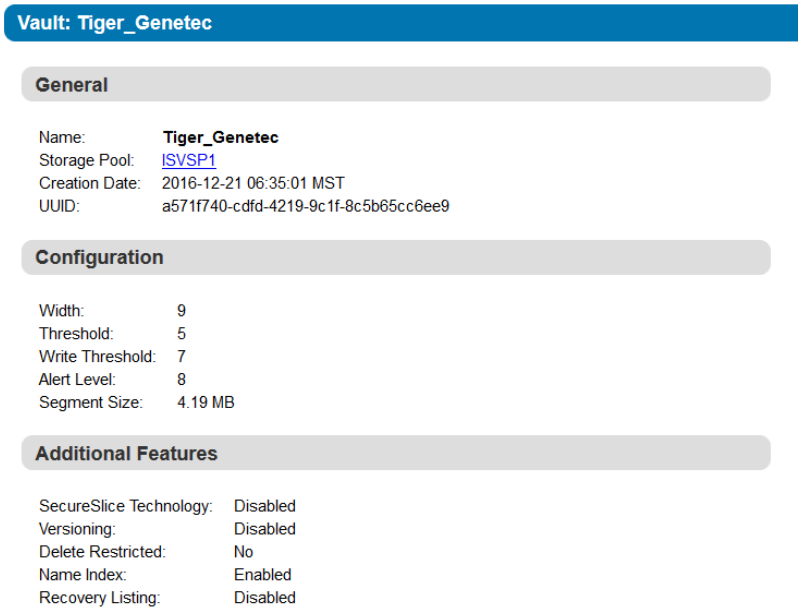


Figure 7: Vault configuration on IBM Cloud Object Storage

10. Create a user and assign the ownership to the vault created in the previous step on IBM Cloud Object Storage.

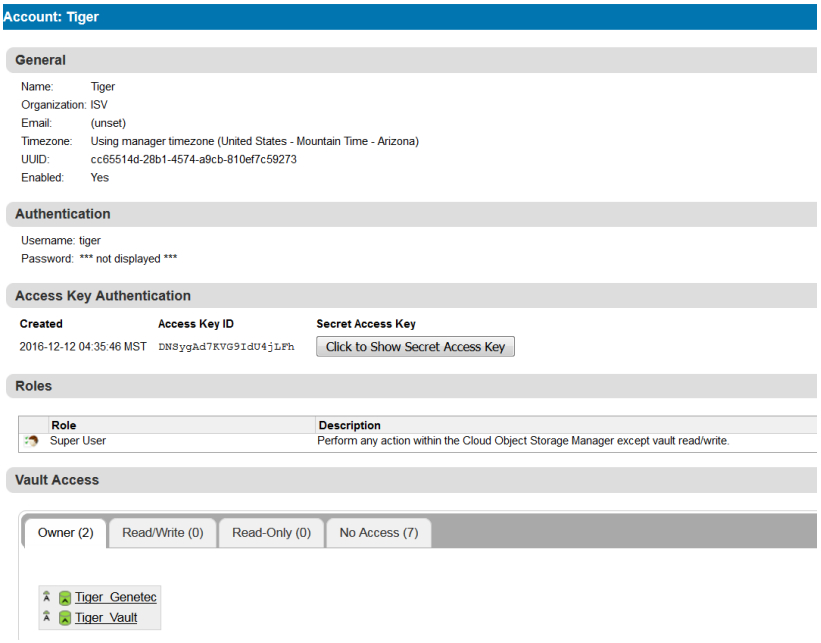


Figure 8: User configuration on IBM Cloud Object Storage

11. Configure the IP address of IBM Cloud Object Storage, vault location details, and user credentials as created in the previous steps for the Tiger Bridge configuration parameters on the Genetec Archiver server.

Test procedure and observations

To validate the transparent data movement between the IBM Storwize system and IBM Cloud Object Storage, various test cases were simulated in the lab to check the sustained throughput under all archiving conditions.

Camera video quality settings include:

- Resolution: H.264 1280x1024
- Frames per second: 20
- Recording frames: All

Test case	Storage throughput	Number of simulated cameras	Number of simulation servers
1 Mbps per camera continuous recording	300 Mbps	300	3
1 Mbps per camera motion detection	100 Mbps	100	2
5 Mbps per camera continuous recording	300 Mbps	60	3
5 Mbps per camera motion detection	150 Mbps	30	2

Table 2: Test simulation configuration details

Tiger Bridge connector was configured to move all the video files except the latest one to the IBM Cloud Object Storage. This can be verified by browsing the files in Windows Explorer.

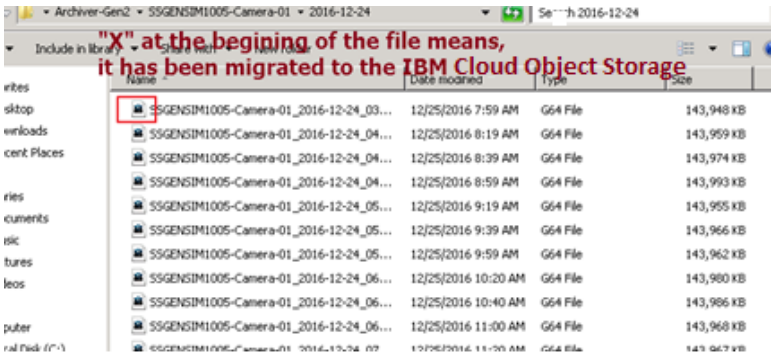


Figure 9: Tiger Bridge connector file movement verification

After camera ingesting ran for a period of 24 hours, the test team logged into the security desk application to monitor the events, such as archiving queue full and pocket loss errors. Security desk was used to request playback streams continuously from the archived storage. Live video caching is disabled for validating the storage video unit performance during playback streams.

The play procedure includes the following steps:

1. Open a 12-camera view in the security desk application for the playback.
2. Use the timeline selector to select the last four hour of video.
3. Increase the playback speed for forward and backward movement.
4. Click **Play**.

The video playback time must span for couple hours of the data that resides in the archiver and needs to be adjusted during the playback streams.

During the 5-day test, up to 300 cameras were simulated with h.264, 20 frames per second, continuous recording or motion detection capabilities.

Storage unit space from the IBM Storwize has been configured on the archiver for storing the video content. Tiger Bridge was configured to move the all the video archived files to the IBM Cloud Object Storage. Play back tests were ran in the continuous loop mode to measure the throughput of Tiger Bridge connector and IBM Cloud Object Storage video unit when the archiver is deleting oldest video files. No **Archiving Queue Full** or **RTP packet lost** messages were noticed during these extended testing in the LAB.

Based on the 300 camera lab test results with no data lost, the IBM Storwize V5030, Tiger Bridge Connector and IBM Cloud Object Storage system can provide a simple and very cost effective video surveillance solution. It is recommended to start with an archiver server configured with a 150-camera count as the base configuration and monitor the parameters before adding the additional cameras, without the risk of losing data.

All video content was received through the 10 Gb interface on the archiver server. During the performance run, the 10 Gb adapter operated at a very low utilization. In a moderate camera count environment, binding multiple 1 Gb adapters might be effective, but this was not tested.

Storage system was connected using dual 16 GB FC connections with multi-pathing software. During the performance run, the 16G B FC utilization was low and 8 GB FC might work for the moderate camera count environment. No SSDs or IBM Easy Tier optimization was considered. This is because the data footprint is a write-once, read-never scenario and does not receive any benefit from an SSD architecture.

Summary

IBM has performed extensive testing with Genetec Security Center, Tiger Bridge from the Tiger Technology, IBM Cloud Object Storage and IBM Storwize family. Depending on your requirements, IBM storage system architecture allow an extremely cost effective scalable solution from few hundred to thousands of cameras.

The solution provides the following key benefits:

Easy to use – The IBM Storwize platform is easy to use, proven in operation, and scales to support your requirements. Tiger Bridge is simple to use connector with minimal configuration, which moves the data transparently between online to cloud storage. It simplifies the administration by consolidating online storage and with long-term Cloud Object storage into a single system

Best in class – This solution provides *best-in-class* and extreme scalable video solutions to enable your business, reduce costs, optimize processes, protect assets, and ultimately increase value in your organization's products and services.

Solution partnership – By combining the innovative solution from the Genetec, and Tiger Technology with the market-leading IBM Storwize platform and IBM Cloud Object Storage, you can provide a comfortable solution that can provide the best-in-class performance and value. The partnership also ensures that a solution investment can provide value for many years to come with the opportunity to upgrade as required while protecting the legacy investment in technology.

Acknowledgments

Special thanks to the Tiger Technology product management and engineering teams in Europe for loaning the software and licenses that enabled the IBM engineering teams to successfully create an operational test environment and run tests to document the results.

Resources

The following links provide the useful references to supplement the information contained in this paper:

- Genetec Security Center documentation
  https://www.genetec.com/
- Tiger Technologies
  http://www.tiger-technology.com/
- IBM Systems on PartnerWorld
  ibm.com/partnerworld/systems
- IBM Redbooks
  ibm.com/redbooks
- IBM Publications Center
  ibm.com/e-business/linkweb/publications/servlet/pbi.wss?CTY=US

About the authors

Dave Taylor is an executive consultant and an architect in IBM Systems Group ISV Enablement Organization. He has more than 25 years of experience working with the IBM System Storage and server platforms. You can reach Dave at dltaylor@us.ibm.com.

Sanjay Sudam is a consultant and an architect in IBM Systems Group ISV Enablement Organization. He has more than 15 years of experience working with the IBM System Storage and server platforms. You can reach Sanjay at Sanjay.Sudam@in.ibm.com.

IBM Systems
3039 Cornwallis Road
RTP, NC 27709

Produced in the United States of America

Please recycle